

FILED
IN CLERKS OFFICE

2004 OCT -2 A 9:12

U.S. DISTRICT COURT
DISTRICT OF MASS.

EXHIBIT 1

AFFIDAVIT OF SPECIAL AGENT COLLEEN FORGETTA

I, Colleen Forgetta, being duly sworn, depose and state:

1. I am a Special Agent with the Department of Homeland Security, Bureau of Immigration and Customs Enforcement (ICE), assigned to the Special Agent in Charge in Boston. I have been a Special Agent for 20 years. As part of my duties, I am currently assigned to investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I attended the Immigration and Customs Special Agent Cross Training Course at the Federal Law Enforcement Training Center which included a segment on Cybercrimes and Child Pornography, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256)¹ in all forms of media including computer media. I have

¹ "Child Pornography means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where - (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . [or] (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." For conduct occurring after April 30, 2003, the definition also includes "(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct." 18 U.S.C. § 2256(8).

also participated in the execution of approximately 100 search warrants involving various criminal offenses.

2. This Affidavit is made in support of an application for a warrant to search the residence of Darren Wilder, located at 5 Valley Road, Dracut, Massachusetts 01826 (the "SUBJECT PREMISES") and a warrant for a 2004 Ford Pickup Truck bearing license plate number MA 50651 registered to Darren Wilder (the "SUBJECT VEHICLE"). The SUBJECT PREMISES to be searched is more specifically described as a single story, single family residence with an attached garage located on a corner piece of property at the intersection of Valley Road and Broad Road. The SUBJECT VEHICLE is more specifically described as orange and black in color.

3. The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography, and violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to receive child pornography in interstate commerce and §§ 2252(a)(1) and 2252A(a)(1), which make it a crime to transport or ship child pornography in interstate commerce.

4. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted and based on my conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography.

5. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252 and 2252A are located at the SUBJECT PREMISES and SUBJECT VEHICLE and within a computer and related peripherals, and computer media found at the SUBJECT PREMISES and in the SUBJECT VEHICLE. Where statements of others are set forth in this Affidavit, they are set forth in substance and in part.

6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence and fruits of violations of federal law, including 18 U.S.C. §§ 2252 and 2252A, as well as property used in committing a crime, as specifically described in Schedule A attached hereto, are currently present at the SUBJECT PREMISES and in the SUBJECT VEHICLE.

7. The instant investigation has revealed that an individual employing the e-mail address vzelkk2n@verizon.net, subsequently identified as Darren Wilder purchased a subscription to a website that was distributing child pornography, and that there is probable cause to believe that evidence of a various child pornography crimes will be located at the SUBJECT PREMISES and in the SUBJECT VEHICLE. Paragraphs 8 and 9 explain technical terms

and concepts related to computers. Paragraphs 10 and 11 explain how computers and computer technology have revolutionized the way in which child pornography is produced, utilized and distributed. The information set forth in paragraphs 12 through 27 provide background concerning the underlying investigation through which the lead to Darren Wilder and the SUBJECT PREMISES was developed. They also provide a general overview of how subscriptions to particular websites offering child pornography were linked to individual purchasers, including Darren Wilder. Finally, paragraphs 28 through 48 describe, more particularly, the investigation of Darren Wilder and the SUBJECT PREMISES and SUBJECT VEHICLE.

The Internet and Definitions of Technical Terms Pertaining to Computers

8. As part of my training and experience as well as discussions with law enforcement officers with experience in cases involving computer use, I have become familiar with the Internet (also commonly known as the World Wide Web or the Net), which is a global network of computers² and other electronic devices that communicate with each other using various means, including

² **Computer:** The term "computer" is defined by 18 U.S.C. § 1030(e)(1) to mean "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

computer that provides resources for other computers on the Internet is known as a server. Servers are known by the types of service they provide, that is how they are configured. For example, a web server is a machine that is configured to provide web pages to other computers requesting them. An e-mail server is a computer that is configured to send and receive electronic mail from other computers on the internet. A client computer is a computer on the Internet that is configured to request information from a server configured to perform a particular function. For example, if a computer is configured to browse web pages and has web page browsing software installed, it is considered a web client.

- b. **Computer system and related peripherals, and computer media:** As used in this affidavit, the terms "computer system and related peripherals, and computer media" refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation

equipment, digital cameras, scanners, in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including, but not limited to, JPG, GIF, TIF, AVI, and MPEG.

- c. **Domain Name:** Domain names are common, easy to remember names associated with an Internet Protocol ("IP") address (defined below). For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards - from right to left - further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the United States government, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the world wide web server located at the United States Department of Justice,

which is part of the United States government.

d. **Internet Service Providers (ISPs) and the Storage of**

ISP Records: Internet Service Providers ("ISPs") are commercial organizations that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name - a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password. ISPs maintain records

("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," see 18 U.S.C. § 2510(17), and the provider of such a service is an "electronic communications service." An "electronic communications service," as defined by statute, is "any service which provides to

users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service." 18 U.S.C. § 2711(2).

- e. **Internet Protocol Address:** Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A

dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next dial-up customer. On the other hand, some ISP's, including most cable providers, employ static IP addressing, that is a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer.

- f. **Log File:** Log files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they

contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

- g. **Modem:** A modem is an electronic device that allows one computer to communicate with another.
- h. **Trace Route:** A trace route is an Internet debugging tool used to document the list of inter-connected computers between two computers on the Internet. A trace route will list the names and IP addresses of computers that provide the physical link between two computers on the Internet. Trace routes are useful tools to help geographically identify where a computer on the Internet is physically located, and usually includes information about the registered owner of computers on the Internet.
- i. **Website:** A website consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

- j. **Website Hosting:** Website hosting provides the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting" means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house their hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

Computers and Child Pornography

10. Based upon my knowledge, training, and experience and the experience and training of other law enforcement officers with

whom I have had discussions, computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography have used membership-based/subscription-based websites to conduct business, allowing them to remain relatively anonymous.

11. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, the development of computers has also revolutionized the way in which

child pornography collectors interact with, and sexually exploit, children. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by child pornography collectors in these ways:

a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

b. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as America Online ("AOL") and Microsoft, which allow subscribers to dial a local number and connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their

own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

c. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache³ to look for "footprints" of the websites and images accessed by the recipient.

d. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 40 gigabytes are not uncommon. These drives can store

³ "Cache" refers to text, image and graphic files sent to and temporarily stored by a user's computer from a web site accessed by the user in order to allow the user speedier access to and interaction with that web site.

thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

Overview of the Underlying New Jersey Investigation

12. The information set forth below is provided as a broad overview of the investigation conducted to date. It does not include a listing of all investigative techniques employed or even the full and complete results of any of the listed investigative efforts.

13. The United States Attorney's Office for the District of New Jersey ("USAO DNJ"), the U.S. Department of Justice's Child Exploitation and Obscenity Section ("CEOS"), and the New Jersey offices of ICE, Internal Revenue Service, Criminal Investigations Division ("IRS CID"), the United States Postal Inspection Service ("USPIS"), and the Federal Bureau of Investigation ("FBI") conducted a joint investigation (the "New Jersey Investigation") of Regpay, a third-party billing and credit card aggregating company. The investigation revealed that Regpay conspired with other website operators to commercially distribute child pornography by providing the other websites with billing and credit card aggregating services, and taking a percentage of the

other websites' illegal proceeds. The investigation also revealed that Regpay itself operated several websites that sold child pornography.

A. Regpay's Billing Service Operations for Child Pornography Websites

14. The New Jersey Investigation revealed that (1) Regpay operated regpay.com, a website that it used to conduct its billing services; (2) the regpay.com website was housed on a server at Verio, Inc.; (3) Regpay leased IP addresses at Rackspace Managed Hosting ("Rackspace"), and Regpay housed its customer databases including customer transaction records on servers at Rackspace; (4) Regpay obtained the assistance of Connections USA, Inc. ("Connections"), which is located in Florida, to coordinate its billing and credit card processing services; and (5) Connections processed at least \$3,000,000 for Regpay between November 1, 2002 and April 30, 2003 including credit card transactions that Connections processed for Regpay through Iserve.com ("Iserve"), an e-commerce company that purportedly provides a variety of payment processing services, including the performance of credit card and check processing, for computer websites that offer membership subscriptions to the public.

15. During the course of the New Jersey Investigation of Regpay, federal agents, acting in an undercover capacity ("the UC Agents"), became paid subscribers/members of websites that used

Regpay as a billing company.⁴ In many instances, when a UC agent subscribed to a website or purchased a membership to a website using a credit card, a billing page automatically appeared on the computer screen, which sought personal and financial information, and revealed that the transaction was being processed by or through Regpay. At the top of the billing page was a logo containing the letters "rp" and the word "regpay," as well as the name of the website to which the undercover agent was seeking to subscribe or purchase. After completing the form, which included providing a credit card number to be used for the purchase, each UC agent was instructed to "hit the JOIN NOW! button" on the screen. Shortly after clicking on the "JOIN NOW!" button, each UC agent received a message from Regpay stating that Regpay successfully charged the provided credit card. The message provided each agent with a transaction number, log-in information, and a password to log into the members-only site. The message stated that "Iserve will appear on your credit card statement as a beneficiary of this transaction." After successfully making the credit card purchase, each UC agent was allowed unlimited access to the members-only portion of the purchased site for a one month period.

16. In some instances, shortly after receiving the above

⁴ The investigation revealed that not all of those websites used Regpay exclusively; some of those websites used multiple billing companies.

described message from Regpay, the agent/purchaser also received a message from "Iserve.com," thanking the customer for using Regpay, and indicating that Iserve would appear on the customer's billing statement. The message thereafter provided the date and time of the transaction, a transaction number, and the amount of the transaction. Records later obtained from the banks that issued the credit cards used in several of the undercover purchases listed "Iserve" for each of these transactions.

17. As part the New Jersey Investigation of Regpay, information housed on various servers that helped facilitate customer transactions for hundreds of websites was seized from several locations in the United States pursuant to several search warrants. After analyzing the customer data, the ICE forensic agents identified tens of thousands of purchases of memberships to websites between January 2003 and July 2003 that had contained child pornography at the time of the UC agent's purchases at specific dates and times between January 2003 and July 2003, that is tens of thousands of confirmed subscriptions which granted purchasers access to those websites.

18. Further, undercover purchases made by ICE agents (described above in paragraphs 15-16) prior to executing search warrants for Regpay's customer transactional information, were found to be recorded in the database found on Regpay's Rackspace server. ICE forensic specialists determined that the Regpay database operated

under a database management system called "MySQL", and that this database's contents and structure were thus legible. In other words, upon finding that the database operated using the MySQL system, and that the coding was intelligible, ICE forensic experts determined that they could decipher Regpay's customer transactional data and use it to identify the subscribers/members of the websites to whom Regpay had provided third-party billing services.

19. At various times between February and September 2003, federal agents verified that at least 21 websites that Regpay had been servicing were still active, accessible on the Internet, and contained child pornography. They did so by accessing these websites on the Internet and subscribing to those sites that advertised child pornography or showed actionable images in their "preview" or "nonmember" sections.

20. Based on the customer transaction records obtained through the execution of search warrants which revealed customer subscriptions to websites that federal agents had independently verified as containing child pornography, the ICE Cyber Crimes Center identified various individuals as subscribers to websites containing child pornography. In turn, the ICE Cyber Crimes Center sent leads to field offices across the country. This search warrant application of the SUBJECT PREMISES and SUBJECT VEHICLE evolved from one of those leads.

B. ICE analysis of Regpay's customer transactional data

21. By way of background, and as noted earlier, Regpay's customer transactional information was found to be recorded in the database found on Regpay's Rackspace server, which was searched pursuant to a warrant. ICE forensic specialists examined the source code⁵ or 'scripts' used to populate the various fields in the Rackspace database, and determined how each of the fields pertaining to the websites' customers (hereinafter, "subscriber(s)/member(s)") were generated by Regpay's web page programming.

22. The ICE forensic specialists learned that when Regpay had served as the billing company for the members-only websites that contained child pornography, the subscribers/members of these websites would input certain information when a billing page would appear. That information was then recorded by Regpay in fields that it maintained in its database.

23. The fields that appeared in the Regpay customer information data, which ICE forensic specialists determined had been completed based upon information provided by the websites' subscribers/members were:

- a. **fname**, referring to the website subscriber/member's first name as entered on the Regpay form;

⁵ Source code is computer software programming statements and instructions.

- b. **lname**, referring to the website subscriber/member's last name of the customer as entered on the Regpay form;
- c. **addr**, referring to the website subscriber/member's street address as entered on the Regpay form;
- d. **city**, referring to the website subscriber/member's city as entered on the Regpay form;
- e. **state**, referring to the website subscriber/member's state as entered on the Regpay form;
- f. **zip**, referring to the website subscriber/member's zip code as entered on the Regpay form;
- g. **phone**, referring to the website subscriber/member's telephone number as entered on the Regpay form;
- h. **country**, referring to the website subscriber/member's country as entered on the Regpay form;
- i. **ccnumber**, referring to the website subscriber/member's credit card number as entered on the Regpay form;
- j. **cvv2**, referring to the website subscriber/member's three digit number from the credit card, as entered on the Regpay form;
- k. **card_type**, referring to the website subscriber/member's credit card, as entered on the Regpay form;
- l. **expmonth**, referring to the website subscriber/member's credit card, as entered on the Regpay form;

m. **expyear**, referring to the website subscriber/member's credit card expiration date, as entered on the Regpay form;

n. **email**, referring to the website subscriber/member's e-mail address as entered on the Regpay form.

24. Federal agents who had subscribed, in their undercover capacity, to one or more websites containing child pornography, and whose transactional information was found to be among the consumer transaction data seized during the searches of Rackspace's Regpay servers, verified that the information pertaining to the transactions they had conducted was contained as each of them had input it in the Regpay database.

25. ICE Cyber Crime Center determined that a field in the "members" table of the Regpay database called "siteid" was a unique identifier that correlated each subscription purchase to a website listed in the "sites" table of the database. ICE agents were able to determine which website each customer purchased by correlating the siteid entry in the "members" table to the relevant "sites" table entry.

26. In addition to determining which fields were completed by subscribers/members, forensic specialists at ICE's Cyber Crime Center also determined that the following fields on the Regpay customer transaction forms were generated automatically by Regpay's coding or script, and then stored in Regpay's MySQL database:

- a. **login**, referring to the access user name;
- b. **passwd**, referring to a randomly generated 8 character password;
- c. **regtime**; referring to the hour:minute:second the script ran (according to the host machine).

27. The fact that the fields referenced in paragraph 26 were computer-generated and were relayed to subscribers/members prior to their entry into the purchased websites is significant. Based on my training and conversations with other agents, although a website subscriber/member could easily provide a false name when subscribing to websites, the subscriber/member most certainly had to provide a legitimate credit card number and e-mail account in order to subscribe to/become a member of the website. This is because the subscriber/member would have been required to provide a valid e-mail account in order to actually enter the website in which s/he was interested. In fact, entry into the members-only websites that contained child pornography must have been preceded by the subscriber/member's receipt of an e-mail that, along with confirmation that the credit card purchase had been successfully completed, included the subscriber/member's computer-generated password, as well as instructions needed to access the website (see paragraph 15). Inaccurate credit card or e-mail information would have precluded entry into the website. Given the likely accuracy of the e-mail address and credit card information

provided by the subscriber/member, federal agents focused on that information to identify subscribers/members.

Probable Cause to Search the Subject Premises

28. Upon receipt of a lead from the ICE Cyber Crimes Center, the undersigned Affiant, working with other agents in the Boston field office commenced an investigation, which revealed that on or about March 15, 2003, an individual whose e-mail address is vzelkk2n@verizon.net, using the name Darren Wilder and using credit card number 5410654922336711, did knowingly and willfully pay for and subscribe to a website (using a computer) later confirmed to contain child pornography. Based on the investigation and my training and experience, there is probable cause to believe that Darren Wilder is a recipient and collector of child pornography, and that evidence of his receipt and possession of child pornography will be found at his residence, the SUBJECT PREMISES.

29. More specifically, in the course of analyzing the Regpay customer transactional data that had been seized pursuant to the search warrants referenced above, it was discovered that an individual using the email address vzelkk2n@verizon.net subscribed to a members-only website, www.lust-gallery.com. The investigation further revealed that the individual using the e-mail account vzelkk2n@verizon.net used a credit card to purchase access to a members-only website on or about March 15, 2003,

specifically, a card issued by Citibank with a card number of 5410654922336711.

30. The members-only site purchased by vzelkk2n@verizon.net permitted electronic access to child pornography.

31. On March 26, 2003, a federal agent, while acting in an undercover capacity, purchased a one-month membership, in the approximate amount of \$49.95 + additional fees, to a website entitled "Lust Gallery," found at www.lust-gallery.com. A credit card number was provided to effect this transaction. The information appearing in the address box of the undercover agent's internet browser while viewing the subscription page was <http://64.239.16.69/sale.cgi?s=91111&ad=ad00094313>. The name "regpay" appeared in relatively large letters on the webpages as the main billing company and on the approval page in smaller type was the name "ISERVE", which was listed as the "beneficiary of this transaction." Additional information on the approval page included the transaction number: 178628, a login: me01793961, a password: 4YHdhagp, and a members URL of <http://69.0.255.118/members/>. Using this information, the undercover agent accessed the website and downloaded images of children engaged in sexually explicit conduct. Contained on the website were numerous pictures depicting minor females in various poses and states of undress. Specifically, three of the images contained on the website are described as follows:

A. 35&back=30: This image features a prepubescent, nude female raising the left leg of a second prepubescent, nude female, exhibiting the genitals of the second prepubescent female.

B. 7&back=0: This image features a closeup of the genital and anal area of a prepubescent nude female with her legs apart exhibiting her genitals.

C. 31&back=30: This image features a closeup of the genital area of a pubescent nude female squatting on the floor with her legs spread apart.

32. On July 24, 2003, another federal agent, acting in an undercover capacity, purchased a one-month membership, for approximately \$57.90, to a website with a URL of www.lust-gallery.com. The undercover agent used an UC credit card, which was provided to a billing company identifying itself as "Regpay." Regpay thereafter provided the undercover agent with a transaction number: 295855, a login: me01901994, a password: 6Sp3Gqmg, and a members URL of <http://69.0.237.226/members>.

Using this information, the undercover agent accessed the website and downloaded images of children engaged in sexually explicit conduct. The home page of the website features images of several females of various poses, and an invitation to become a member of the website. Contained within the website were numerous pictures of young girls in various poses and states of undress.

Specifically, three of the images contained in this website when accessed by this undercover agent are described as follows:

A. **Photo 2400 of 9833 (Set #8):** This image features a frontal view of a prepubescent female and another minor female, who are sitting on a wooden table. The left most female is sitting on the table leaning back on her hands slightly, her legs bent at the knees and are spread apart exposing both her genital and anal region. Her undeveloped breasts are also exposed.

B. **Photo 7508 of 9833 (Set #23):** This image features two prepubescent females. The right most female is lying partially on her back on what appears to be a multi-colored cover on top of a mattress on the floor. Her legs are extended over her head and her toes are touching the floor, above her head, her legs are parted and both her genital and anal region is exposed. The left most female is sitting on the mattress, her left leg is bent at the knee, resting it on the mattress, parallel to the floor. The right leg is bent up at the knee and the female is leaning forward, leaning her upper bodice on her thigh. The photo was taken from a frontal viewpoint.

C. **Photo 208 of 9833 (Set #1):** This image features two minor females. The two minor females are on a bed, and are on their hands and knees facing away from the view point of the camera. Both minor females have their legs parted, exposing their genital and anal region.

33. The undersigned Affiant reviewed a hard drive, which contained digitally preserved copies of the above-listed website purchased by undercover agents on July 24, 2003, that was sent to my ICE field office. The undersigned Affiant has also personally reviewed the content of the above website, purchased by vzelkk2n@verizon.net that were digitally preserved and the content copied to the hard drive by ICE Agents at the Cyber Crimes Center in Fairfax Virginia. Law enforcement officers with expertise in the field of child pornography reviewed several images from each of those websites and concluded that they constitute child pornography.

34. In addition, the undersigned Affiant reviewed the preview page of www.lust-gallery.com, as preserved by law enforcement on March 26, 2003, and found the following: The top of the page states "LUST GALLERY - a Secret Lolitas Archive". It is followed by text stating: "That you're here means you're a member of one of the sites created by RedStudio. This website was developed exclusively for our members and will never be revealed to the general public. Because you were a subscriber before, we know what you like and need. And we're here to give EXACTLY the things you like EXACTLY the way you like them." This text is followed by thumbnail photos appearing one after the other across the width of the screen. Each image shows at least two unclothed minors with some images focused on the minor's genitalia. After

the first row of images further text appears and states "Lust Gallery contains thousands of EXCLUSIVE images never published before. Moreover, inside we have something THAT HAS NEVER BEEN SHOWN BEFORE UNTIL NOW!" This text is followed by another paragraph stating: "All models inside are 14 or younger, every image shows at least 2 or 3 girls, every gallery is at least 50 images. Currently we have over 3500 high quality digital photos in over 40 sets. The collection is updated weekly so there is always something new for you to enjoy. Created by real young model lovers for real young model lovers. Lust Gallery is truly an elite product. We guarantee you complete satisfaction for a truly unforgettable experience." This text is followed by another row of thumbnail images going across the width of the screen. Each image shows at least two unclothed minors with some images focused on the minor's genitalia. Further text follows these images. As noted above, the preview page is what a customer would typically see before deciding to purchase or subscribe to the website.

35. Verizon is an ISP through which the email account vzelkk2n@verizon.net was issued. Records from Verizon reveal that the e-mail address vzelkk2n@verizon.com is assigned to Darren Wilder whose billing address is 5 Valley Road, Dracut, Massachusetts 01826 (the SUBJECT PREMISES).

36. Verizon also confirmed that Darren Wilder's account was activated on November 22, 2002; that the account was active at the time of the purchase described above and is still active.

37. Furthermore, information from Citibank, the credit card company that issued a credit card used to make the purchase described above, reveals that Darren Wilder is the account holder, and that his billing address at the time of the above described purchase was 551 Hildreth Street, Dracut, Massachusetts, 01826. The records from Citibank further reveal the following purchase, among others:

Date	Ref. No.	Description of Transaction	Amount
03/15/ 03	CSPJ02T1	ISERVE *8009290300 800-929- 0300 FL	\$57.90

The credit card purchase on March 15, 2003 corresponds with the date that vzelkk2n@verizon.net purchased access to www.lust-gallery.com as listed in the leads sent by the Cyber Crimes Center that were taken from Regpay's customer database, and list Iserve as the beneficiary of the transaction. Based on the verification of undercover transactions described above in paragraphs 15-16, agents determined that the credit card purchases correspond with other purchases as reflected in the customer transaction records maintained by Regpay on the Rackspace servers, and fell either on the exact day or one day before the recorded purchase.

38. Additional investigation of Darren Wilder revealed that he has a prior criminal conviction in the United States District Court for the District of Massachusetts for possession of child pornography in violation of Title 18, United States Code, Section 2252A(a)(5)(B). On November 9, 2000, Darren Wilder was sentenced in that case to 27 months incarceration, followed by two years of supervised release. The underlying specific allegations for this prior offense were that between December 1999 and January of 2000, Wilder, using a computer, arranged to purchase through an undercover website a videotape containing child pornography. The videotape was advertised on the undercover web site as illegal material containing images of child pornography specifically depicting a 12 year old girl. At the time of delivery of the videotape ordered by Wilder, law enforcement officers had a search warrant to search his residence. The search warrant execution revealed that Wilder was in possession of fourteen computer disks containing numerous images of child pornography, including graphic images of minors engaged in sexually explicit conduct. Wilder admitted to law enforcement officers at that time that he collected these images off the Internet over a several year period of time.

39. On November 1, 2002, Wilder was released from incarceration on his child pornography sentence and placed on supervised release. As of the date of this affidavit, Wilder is currently

on supervised release. Wilder's United States Probation Officer ("P.O.") is Craig Orze, from the District of Massachusetts with an office address of 499 Essex Street, Suite 3, Lawrence, Massachusetts.

40. P.O. Orze reports the following: On or about November 1, 2003, Wilder moved from 551 Hildreth Street, Dracut, Massachusetts to 5 Valley Road, Dracut, Massachusetts (the SUBJECT PREMISES). P.O. Orze has been to the SUBJECT PREMISES on a number of occasions and as recently as November 19 and December 30, 2003. While at the SUBJECT PREMISES, P.O. Orze observed that Wilder still has a computer which he observed to be located in a spare bedroom/office room in the residence. In addition, P.O. Orze has had numerous conversations with Wilder specifically confirming that he has Internet access at home, as it is needed for Wilder to continue in his occupation as a Mac Tools salesperson. Wilder also informed P.O. Orze that in addition to his desktop computer he has a laptop (portable) computer that P.O. Orze observed on November 19, 2003 to be in the SUBJECT VEHICLE and on December 30, 2003 to be in the SUBJECT PREMISES. Wilder further informed P.O. Orze that he uses the laptop computer when he travels for business. The SUBJECT VEHICLE was subsequently identified as a 2004 Ford Pickup Truck bearing license plate number MA 50651. P.O. Orze also confirmed

Wilder lives alone at the SUBJECT PREMISES and that he works from his residence.

41. Information provided by the Massachusetts Electric Company has identified the holder of an electric utilities account for services provided at the SUBJECT PREMISES as Darren Wilder. The service was established on October 29, 2003.

42. As of January 7, 2003, information obtained from the Commonwealth of Massachusetts indicates that Darren Wilder has a Massachusetts driver's license indicating an address of 5 Valley Road, Dracut, Massachusetts (the SUBJECT PREMISES).

43. On December 23, 2003 and January 8, 2004, your Affiant drove by the SUBJECT PREMISES and observed the SUBJECT VEHICLE, a 2004 Ford Pickup Truck located in the driveway of the SUBJECT PREMISES bearing a license plate number of MA 50651. Information obtained from the Commonwealth of Massachusetts, Registry of Motor Vehicles revealed that it is registered to Darren Wilder.

44. Information obtained from Verizon indicates that Wilder currently subscribes to Internet services from Verizon and has a billing address of 5 Valley Road, Dracut, Massachusetts 01826 (the SUBJECT PREMISES) and that the service is active. In addition, Verizon records reveal an assigned email address of vzelkk2n@verizon.net.

45. Based upon the information provided by P.O. Craig Orze, Verizon, Massachusetts Electric Company and the Commonwealth of

Massachusetts, this Affiant believes that the individual using the email address of vzelkk2n@verizon.net is Darren Wilder, who lives at the SUBJECT PREMISES and owns the SUBJECT VEHICLE.

46. Based upon my training and speaking with Special Agent and Group Supervisor, John MacKinnon of ICE, whose background includes having been a special agent with ICE/U.S. Customs for 15 years, and participating in over 200 child pornography investigations over the past 8 years, participating in over 50 searches relating specifically to child pornography offenses, and having instructed over 7,000 law enforcement officers specifically on conducting child pornography investigations, as well as my discussions with other law enforcement officers with experience in the area of child exploitation, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the

inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Collectors of child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica,⁶ and video tapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact

⁶ "Child erotica," as used in this Affidavit, is defined as materials or items that are sexually arousing to certain individuals but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

and who share the same interests in child pornography.

f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

47. The undersigned Affiant submits that there is probable cause to believe that Darren Wilder, utilizing Internet access through Verizon, at 5 Valley Road, Dracut Massachusetts, (SUBJECT PREMISES) is a collector of child pornography. This opinion is based in part upon the following:

- (a) Darren Wilder's purchase of a membership to a child pornography website;
- (b) Wilder's prior criminal conviction for possession of child pornography in November of 2000;
- (c) Wilder's prior use of a computer to order child pornography;
- (d) The preview page of the website membership purchased by Wilder indicating the nature of the images on the website for which he subscribed - sexually explicit pictures of young girls - 14 and under.

48. Finally, based upon the conduct of individuals involved in the collection of child pornography set forth above in paragraph 43, namely, that they tend to maintain their collections at a secure, private location for long periods of time, there is probable cause to believe that evidence of the offenses of

receiving and possessing child pornography is currently located at the SUBJECT PREMISES.

Specifics Regarding the Seizure and Searching of Computer Systems

49. Based on my own experience and consultation with other agents who have been involved in the search of computers and retrieval of data from computer systems and related peripherals, and computer media, there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer experts in a laboratory or other controlled environment:

a. Computer storage devices, such as hard disks, diskettes, tapes, laser disks, can store the equivalent of hundreds of thousands of pages of information. Additionally, when an individual seeks to conceal information that may constitute criminal evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This review and sorting process can take weeks or months, depending on the volume of data stored, and would be impossible to attempt during a search on site; and

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in some systems and applications.

It is difficult to know before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

50. Based on my own training and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs

the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

c. I am familiar with and understand the implications of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the SUBJECT PREMISES are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

Conclusion

51. Based on the above information, I believe probable cause exists to conclude that Darren Wilder has violated various provisions of 18 U.S.C. §§ 2252 and 2252A, relating to child pornography, and that there exists evidence, fruits and instrumentalities of the above identified crimes located at the

SUBJECT PREMISES and in the SUBJECT VEHICLE, as more fully described in Schedule A attached hereto.

Colleen Forgetta
Special Agent, ICE

Subscribed and sworn to before me this 14th of January 2004.

ROBERT B. COLLINGS
United States Magistrate Judge

EXHIBIT 2

AO 106 (Rev. 7/87) Affidavit for Search Warrant

United States District Court

DISTRICT OF MASSACHUSETTS

In the Matter of the Search of

(Name, address or brief description of person, property or premises to be searched)

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 2004 M 0431 RBC

the residence of Darren Wilder, located at 5 Valley Road,
Dracut, Massachusetts 01826, more specifically described
as a single story, single family residence with an

attached garage; and the 2004 Ford pick-up truck,
bearing MA registration 50651, registered to Darren Wilder
Colleen Forgetta

being duly sworn depose and say:

I am a(n) _____ Special Agent, I.C.E. _____ and have reason to believe
Official Title

that ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

the residence of Darren Wilder, located at 5 Valley Road, Dracut, Massachusetts 01826, more specifically described
as a single story, single family residence with an attached garage; and the 2004 Ford pick-up truck, bearing MA
registration 50651, registered to Darren Wilder

in the _____ District of _____ Massachusetts

there is now concealed a certain person or property, namely (describe the person or property to be seized)
see Schedule A attached hereto

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)
property that constitutes evidence of a criminal offense, contraband and things otherwise criminally possessed and
property that has been used as a means of committing a criminal offense

concerning a violation of Title _____ 18 _____ United States code, Section(s) _____ 2252 and 2252A

The facts to support a finding of Probable Cause are as follows:

see attached affidavit of Colleen Forgetta

Continued on the attached sheet and made a part hereof.

☒ Yes☐ No

Sworn to before me, and subscribed in my presence

2004 JAN 14 2004

Date

ROBERT B. COLLINGS

UNITED STATES MAGISTRATE JUDGE

Name and Title of Judicial Officer

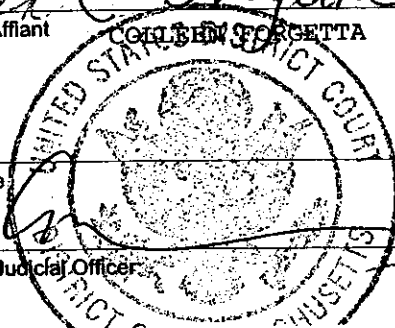
This form was electronically produced by Elite Federal Forms, Inc.

at Boston, MA
City and State


Signature of Judicial Officer

Signature of Affiant


COLLEEN FORGETTA



SUBJECT PREMISES and in the SUBJECT VEHICLE, as more fully described in Schedule A attached hereto.



Colleen Forgetta
Special Agent, ICE

Subscribed and sworn to before me this 14th of January 2004.


ROBERT B. COLLINGS
United States Magistrate Judge

I have viewed the
images denoted 7 & back = 0
and 31 & back = 30 and find that
they depict minors engaged
in "sexually explicit conduct"
specifically, "provisions exhibition
of the genitals" of the minors.
18 USC § 2256 (1)(2)(E).

JAN 14 2004


usm J